CA Liability

Federal PKI Technical Working

March 8, 2001

Agenda

- What is Trust

Introduction to Trust

- Technology and Trust are Different
- Natural Technology Providers
- Natural Trust Providers
  - Clergy
  - Doctors
  - Institutions of Higher Learning
  - Financial Institutions

What is Trust?

- Trust is Earned or Bestowed not Claimed
- Function of Esteem or Authority
- Function of Policies, Procedures, & Controls
- Function of Oversight
- Function of Willingness to Assume Responsibility / Liability (Moral or Fiscal)

Authentication Over the Internet

- Since you can't be there…
- Need to send something that belongs to you and only you (Unique Identifier)
- What if you could send your fingerprint?
- Hi, my name is Scott Lowry, this is my fingerprint, trust me!
- Those days are gone…

What Would Be Needed for This Model to Work?

- Someone would have to meet me
  - Examine my identity credentials
  - Examine my finger print
  - Somehow bind my identity to my fingerprint
- Be willing to make a representation that:
  - Anyone who receives a message with my finger print attached could reasonably assume that the message came from me

That Someone Is a Certificate Authority aka CA

- Acting as trusted third parties, CAs link a unique identifier to an individuals identity.
  - Unique identifier is known as “Public Key”
  - Quality of linkage based upon standing of certificate authority.
  - There is a difference between CAs
    - Dingbat flower shop vs.
    - Federal Reserve Bank.

Digital Certificate: The Electronic Proof of Linkage

- Electronic manifestation of the linkage between individual's identity and individual's public key

Lessons from the Credit Card World

- "The map is not the territory"
  - S.I. Hayakawa
- What is a Credit Card?
  - What turns plastic into money?
  - What makes credit cards portable?
- What Does "VISA on the Front" Really Mean?
  - Represents contract infrastructure all parties have agreed to play by

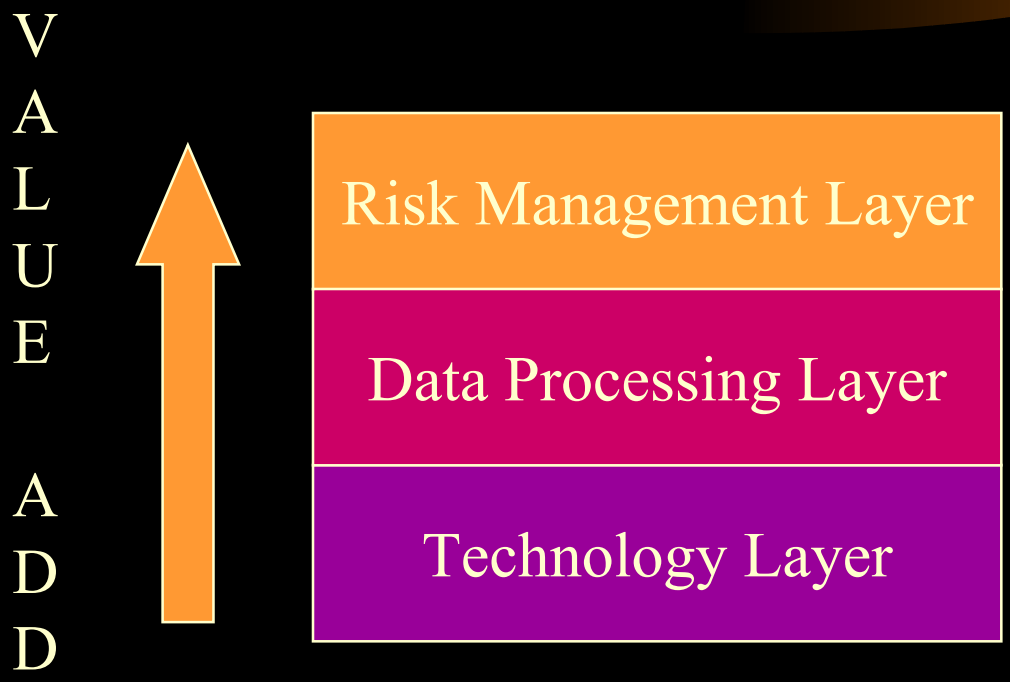
Digital Certificate Players & Their Roles

Policy Authorities	Accreditors	Certificate Authorities	Certificate Manufacturers	Relying Parties
Government • GSA ACES	**Big "X"** • SAS 70 •Web CA	**Government**	•**Technology Providers** •**Service providers**	**Government** •B2G •C2G •G2G
Financial Institutions • ABA TrustID	**Government** • FIPS 140 • CC	**Financial Institutions**	**ASPs**	**Business** •B2B •B2C
Healthcare • Medtegrity	**Standards Bodies** •ANSI	**Industry Consortia**	**CAs**	**Consumers** •**C2C**

What Is a Digital Certificate (Really)

- Manifestation of Rights & Privileges Accorded to It by Those Who Accept It.
- Rights & Privileges Function of Who Accepts Certificate and for What Purposes
- Those Who Accept Certificates Known as "Authorized Relying Parties"

Digital Certificate Value Chain



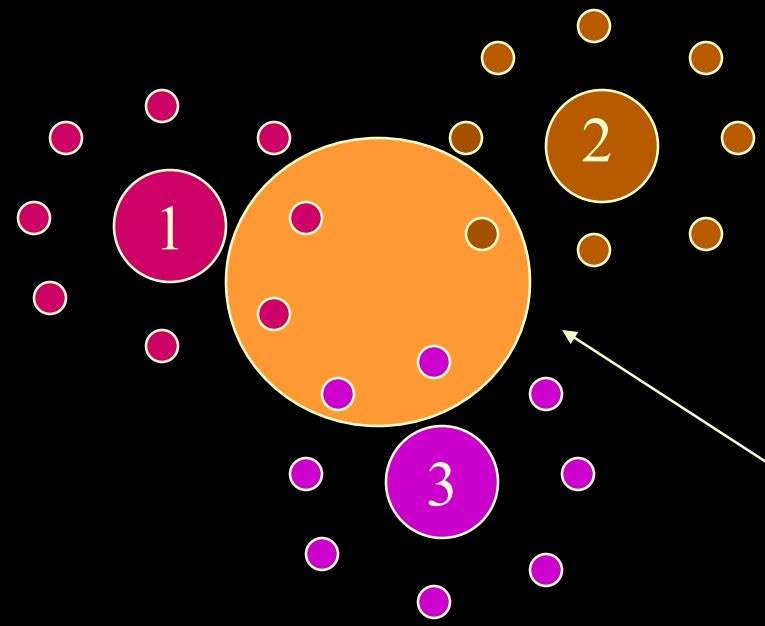
The Implications of All This

- Coming Soon to a Web Site Near You
  - "We Accept the following Digital Certificates"
- It Won't be 50, 20, or 10; It Will be 3 to 5

What to Do About Digital Certificates

- Digital Signatures Require Digital Certificates
- Two Alternatives
  - Issue Your own Certificates
    - In-Source or Out-Source Manufacturing
  - Accept Someone Else's Certificates

The Problem With the Enterprise CA Model



Customers that will require multiple certificates

1 = Enterprise CA

= Enterprise Customers

The Merits of Accepting Someone Else's Digital Certificates

- Avoids Need for Multiple Certificates
- Minimizes Number of Rule Sets
- Reduces Exposure to Risk and Liability
- Cheaper Overall Systems Costs

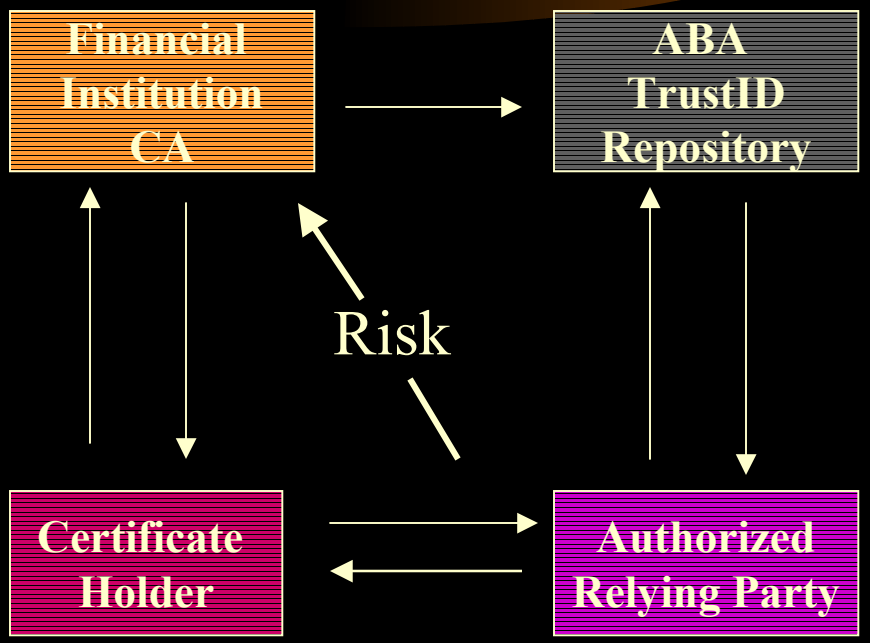
Determining Whose Certificates to Accept

- It's a policy issue not a technology issue
- Whose rules will you accept
- Contract infrastructure defines the rules
- Critical issue is liability
  - What happens if the CA gets it wrong
- Liability for inaccurate certificates and/or sloppy operations critical issues

TrustID Risk Transfer Model

Risks Transferred:

1. **CA Technology**
2. **CA Operations**
3. **Repository Operations**
4. **Identity & Authentication**
5. **Certificate Revocation**
6. **Third Party Liability**



Certificate Authorities & Internet Transaction Risk

- Operations
- Authentication
- Performance
- Velocity

For More Information

J. Scott Lowry
President & CEO
Digital Signature Trust Co.
801-246-4351 (o)
801-554-0430 (c)
scott.lowry@trustdst.com